Factoring numbers with a single interferogram

Vincenzo Tamma[1,2], Heyi Zhang[1], Xuehua He[1], Augusto Garuccio[2], Wolfgang P. Schleich[3], and Yanhua Shih[1]

[1]*Department of Physics, University of Maryland, Baltimore County,*
Baltimore, Maryland 21250, [2]*Dipartimento Interateneo di Fisica,*
Università degli Studi di Bari, 70100 Bari, Italy,
[3]*INFN Sezione di Bari, Bari, Italy,* [4]*Institut für Quantenphysik,*
Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany

We construct an analogue computer based on light interference to encode the hyperbolic function $f(\zeta) \equiv 1/\zeta$ into a sequence of skewed curlicue functions. The resulting interferogram when scaled appropriately allows us to find the prime number decompositions of integers. We implement this idea exploiting polychromatic optical interference in a multi-path interferometer and factor seven digit numbers. We give an estimate for the largest number that can be factored by this scheme.

To find the factors of a large integer number N is a problem of exponential complexity. Indeed, the security of codes relies on this fact but is endangered by Shor's algorithm [1], which employs entanglement between quantum systems [2]. In the present paper we report the optical realization of a new algorithm for factoring numbers, which takes advantage of interference only.

A naive way of approaching the problem of factorization consists of dividing N by integers ℓ, starting from $\ell = 3$ until N/ℓ is an integer. In the worst case this procedure requires $\sqrt{N}$ divisions before one would find a factor. On a digital computer division of large numbers is a rather costly process. However, in many physical phenomena division occurs in a rather natural way. For example, a wave of wavelength λ, propagating over a distance L, acquires a phase $\phi = 2\pi L/\lambda$ and therefore probes the ratio L/λ. In the optical domain λ is measured in nanometers (nm), that is $\lambda = \ell$ nm. When we also express the path length L in units of nm, that is $L = N$ nm, the phase $\phi = 2\pi N/\ell$ is sensitive to the ratio N/ℓ. For factors of N, ϕ is an integer multiple of 2π. Otherwise ϕ is a rational multiple of 2π.

In order to enhance the signal associated with a factor relative to the ones corresponding to non-factors, we use interference of waves, which differ in their optical path length by an integer multiple. In this way we take advantage of constructive interference when ℓ is a factor of N, but destructive interference when ℓ is not a factor of N. The cancellation of terms is most effective when the individual optical paths increase in a nonlinear way. In this case, the intensity of the interfering waves is determined by the absolute value squared of a truncated exponential sum [3]. A polychromatic source of light, which contains several wavelengths $\lambda = \ell$ nm, allows us to test several trial factors simultaneously, taking advantage of the properties of truncated exponential sums [4] with continuous arguments.

Our method is motivated by recent work on factorization using truncated exponential sums [5], which has been realized in several experiments [6]. However, it differs from the past realizations in three important points:(i) the division of N by the trial factors ℓ is not precalculated [7], but it is performed by the experiment it-
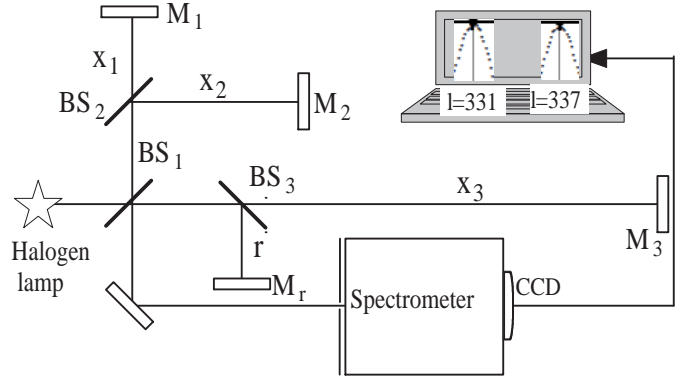

FIG. 1: Experimental setup for factoring numbers using classical interference in a generalized symmetric Michelson interferometer with $M + 1$ paths. This analogue computer consists of a polychromatic source (halogen lamp), M balanced beam splitters, $M + 1$ mirrors, and a spectrometer connected to a CCD camera. The M interfering paths are varied with respect to the reference path of length r, defined by the reference mirror M_r and indicated by thin vertical dashed lines, by displacing the M mirrors. The length of the m-th arm reads $x_m = r + (m - 1)^2 x$, with the unit of displacement x and $m = 1, 2, ..., M$. Here we depict the case $M = 3$.

self, (ii) all the trial factors are tested simultaneously in a single experiment, and (iii) a scaling property inherent in the recorded interferogram of a single number allows us to obtain the factors of several numbers.

The optical setup used to implement this idea is a symmetric Michelson interferometer with $M + 1$ paths in free space shown in Fig. 1 for $M = 3$. In order to calibrate the interferometer the mirrors are arranged such that the path lengths are identical to the length r of the reference path. Next we displace these mirrors in a nonlinear way as to obtain the final path length $x_m \equiv r + (m - 1)^2 x$ of the m-th arm. Here x denotes the unit of displacement. The preparation of the interferometer is completed after we have blocked the reference mirror.

The intensity in the exit port of the interferometer is given by the interference of the waves in the remaining

M arms. Since we deal with balanced beam splitters all waves have the same amplitude. However, due to the different arm lengths x_m of the interferometer the phases $\phi_m = 2\pi x_m/\lambda = 2\pi r/\lambda + 2\pi(m-1)^2 x/\lambda$ give rise to the intensity

$$I(\lambda; x) = |s(\frac{x}{\lambda})|^2, \tag{1}$$

which we have expressed by the curlicue function [8]

$$s(\xi) \equiv \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i(m-1)^2\xi\right]. \tag{2}$$

Here we have normalized the output intensity with respect to the source intensity. Moreover, the reference phase $\phi_r \equiv 2\pi r/\lambda$ which is independent of m has dropped out due to the fact that the intensity in Eq. (1) involves the absolute value squared of the sum s.

From Eq. (2) we note that $|s|^2$ has a dominant maximum at $\xi = 0$ with $s(0) = 1$ and decaying oscillations on the sides. Moreover, we recognize the periodicity property $s(\xi + 1) = s(\xi)$. Therefore, it suffices to consider $s = s(\xi)$ in the interval $-1/2 \leq \xi \leq 1/2$. In addition $|s(\xi)|^2$ is symmetric with respect to $\xi = 0$.

We now consider the dependence of the intensity I given by Eq. (1) on the wavelength λ for a fixed unit x of displacement. The argument ξ of s is the ratio $x/\lambda = k(\lambda; x) + \tau(\lambda; x)$, which we represent by the sum of the integer k and the correction term τ with $-1/2 \leq \tau \leq 1/2$. For a fixed value of x, k and τ depend on λ. It is this dependence of $I = I(\lambda; x)$ on λ which contains the information about the division by λ. Indeed, whenever λ is such that $s = 1$ we find $\tau = 0$ and hence $x/\lambda = k$, which implies that λ is a factor of x.

Since x and λ only enter into the intensity as a ratio we find immediately the scaling law

$$I(\lambda; x) = I(N\frac{\lambda}{x}; N), \tag{3}$$

which suggests that we can find the factors of N by rescaling the interferogram as a function of the dimensionless variable

$$\xi_N \equiv N\frac{\lambda}{x}. \tag{4}$$

Hence, we can exploit the wavelength λ as well as the unit of displacement x to scan the possible trial factors in the interval $1 \leq \xi_N \leq \sqrt{N}$. In principle, by choosing a suitable value of x and an appropriate interval of wavelengths we can factor any large value of N.

It is illuminating to compare our method to factor numbers to Shor's algorithm [1]. Both implement a function. We use a physical system, that is, a classical analogue computer to obtain the continuous function $f(\zeta) \equiv 1/\zeta$. Shor's method takes advantage of the exponentially large Hilbert space of a quantum system to encode the discrete function $g(i) \equiv a^i mod N$ whose period shares a common factor with N. In contrast, we

exploit the very change of the periodicity induced by the function $1/\zeta$ in the interferogram consisting of a sequence of skewed curlicue functions.

We now turn to the experimental implementation of our technique based on a symmetric Michelson interferometer with $M = 3$ beam splitters and four mirrors. Each mirror is mounted on a single axis translation stage which consists of a 5 mm manual travel stage, a 50 mm step motor, and 20 μm piezoelectric and feedback control stage with a resolution of 10 nm.

The polychromatic source of the interferometer is a halogen lamp with a bandwidth ranging from 400 nm to 800 nm. The interference pattern at the output port is measured by a spectrometer [9] connected to a 2048 pixels Charge-Coupled Device (CCD) array of resolution $0.005 - 0.006$ nm, as a continuous function of the wavelengths λ associated with the polychromatic source. The spectrometer and the CCD can cover a range in wavelengths of the order of the light source. An accuracy of the order of 0.006 nm in a single pixel requires the use of a CCD bandwidth of 13 nm.

The calibration of the interferometer with a suitable accuracy is one of the challenging tasks in this experiment. We first determine when all path lengths x_m are equal to r, by measuring the polychromatic two-path interference between the m-th beam and the reference beam, for each $m = 1, 2, 3$, with the mirror M_r tilted by a small angle with respect to all the other mirrors. Then we block the mirror M_r and obtain non-linear interfering path lengths by translating each mirror M_m with the piezoelectric translators combined to the step motors. Our experiment uses the displacement unit $x = 523426.8$ nm.

In the center of Fig. 2, we show the resulting interferogram as a function of the wavelength λ in the interval [460.36 nm, 463.24 nm]. Next we use this pattern to factor two distinct numbers. We start with $N = 1308567 = 1131 \times 1157$ and present towards the bottom of Fig. 2 an axis with the variable ξ_N rescaled according to Eq. (4). We clearly identify the factor 1157 by the maximum being located [10] at an integer, as shown by the inset. Moreover, we use the same interferogram to factor the number $N' = 1306349 = 1133 \times 1153$. For this purpose we show on the top the rescaled variable $\xi_{N'}$. Again we can identify the factor 1153 by the maximum being located at an integer.

What is the range of wavelengths necessary to factor a given number N? The answer to this question emerges from the condition that the spectrum must cover all test factors ranging from 1 to $\sqrt{N}$, that is $1 < \xi_N < \sqrt{N}$ together with the scaling transformation Eq. (4) which translates into the wavelength requirement $1/N < \lambda/x < 1/\sqrt{N}$. Hence, for a given wavelength range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ we can factor numbers N from the interval

$$N_{min} \equiv (\frac{x}{\lambda_{max}})^2 \leq N \leq \frac{x}{\lambda_{min}} \equiv N_{max}, \tag{5}$$
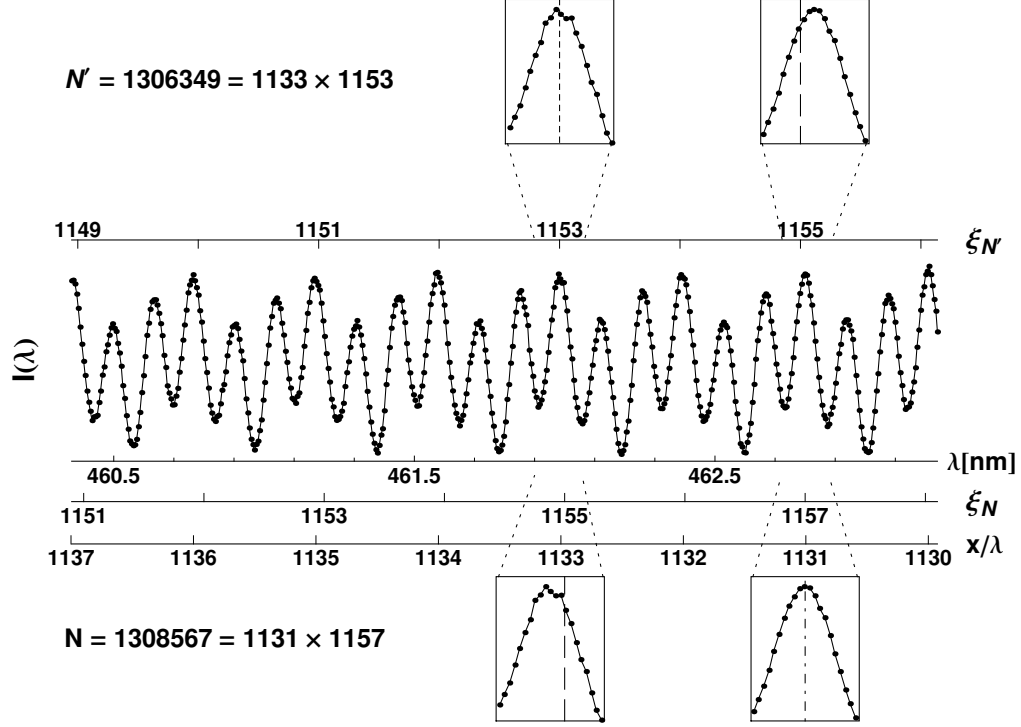
We emphasize that this inequality also puts a re-

FIG. 2: Experimental interferogram $I = I(\lambda;x)$, obtained by the multi-path Michelson interferometer of Fig. 1, for a unit of displacement $x = 523426.8$ nm, in the wavelength range 460.36 nm$\leq \lambda \leq$ 463.24 nm (center) and factorization of the two numbers $N = 1308567 = 1131 \times 1157$ (bottom) and $N' = 1306349 = 1133 \times 1153$ (top), by rescaling the wavelength axis according to Eq. (4). The dots represent the measured values and the curve is obtained by joining the experimental points. The insets magnify the behavior of the interferogram in the neighborhood of the three trial factors 1153, 1155, and 1157 whose locations are indicated by dotted, dashed and dashed-dotted lines, respectively. Only when the dominant maximum in the interferogram is located at an integer we have a factor of N or N'. Every dominant maximum corresponds to a factor x/λ as indicated by the horizontal axes at the bottom.

striction on the displacement x. Indeed, in order to have $N_{min} \leq N_{max}$ we need to satisfy the condition $(x/\lambda_{max})^2 \leq x/\lambda_{min}$, which implies

$$x \leq \frac{\lambda_{max}^2}{\lambda_{min}}. \tag{6}$$

According to Eq. (5) the largest possible number that can be factored is given by the maximum value of x which translates with the help of Eq. (6) into

$$N_{max} = (\frac{\lambda_{max}}{\lambda_{min}})^2 \equiv \beta^2. \tag{7}$$

With the wavelength domain of the halogen lamp we find from Eq. (7) the value $N_{max} = 4$.

This conservative estimate originates from the constraint that we have to cover a wavelength domain large enough to include all test factors up to $\sqrt{N}$. Nonetheless we can still find the factors of some numbers as demonstrated by Fig. 2. Indeed, each dominant peak

in the interferogram corresponds to a factor p of a number $N = p \cdot q$. Since the scaling law Eq. (4) predicts $\xi_N = N\lambda/x = p \cdot q\lambda/x$ that is $q = x/\lambda$ the spectral range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ allows us to determine the factors

$$q_{min} \equiv \frac{x}{\lambda_{max}} < q < \frac{x}{\lambda_{min}} \equiv q_{max}. \tag{8}$$

In order to illustrate this feature we have included in Fig. 2 a horizontal axis on which we mark the possible factors q given by the maxima of the curlicue function.

One possibility of circumventing the bandwidth limitation given by Eq. (7) consists of repeating the experiment for different values of the unit x of displacement while maintaining the bandwidth expressed by the dimensionless parameter β. For a given integer N to be factored we choose n suitable values of $x = x_i$, with $i = 0, 1,, n - 1$ in order to cover subsequent intervals $[\xi_N^{(i)}, \xi_N^{(i+1)}]$ of test factors with $\xi_N^{(i)} \equiv N\lambda_{min}/x_i$ such that $[\xi_N^{(0)}, \xi_N^{(n)}] = [1, \sqrt{N}]$. We achieve this goal provided $x_{i+1} = x_i/\beta$, with $x_0 \equiv N\lambda_{min}$, and $n \lesssim log_\beta \sqrt{N}$ num-

ber of interferograms.

Similarly, we can factor any number in the interval $N_{min} < N < N_{max}$ by using $n \lesssim log_\gamma \sqrt{N_{max}}$ interferograms provided $\gamma \equiv N_{min}/N_{max}\beta > 1$. Such interferograms are obtained for values x_i such that $x_{i+1} = x_i/\gamma < x_i$ with

$$x_0 \equiv N_{max}\lambda_{min}. \tag{9}$$

For example, for factoring all the integers N such that $N_{max} = 10N_{min}$ it would be enough to exploit a wavelength bandwidth $\beta = 20$ in order to achieve the value $\gamma = 2$.

In conclusion, we have outlined and verified by an experiment a new approach towards factoring numbers with the help of a multi-path Michelson interferometer where the individual optical path lengths increase quadratically leading to Gauss sums. However, we could have easily implemented any other polynomial increase where an exponential sum determines the output intensity of the interferometer. We have factored different numbers with up to seven digits from a single recorded interferogram exploiting a remarkable scaling property.

Our experiment relied on only $M = 3$ interfering paths. However, for larger numbers to be factored it can be useful to increase either the number of paths M or the polynomial order of the interferograms in order to obtain sharper peaks and better accuracy in the value of the maxima. A standard best fitting procedure [10] would allow us, in principle, to achieve the necessary accuracy even exploiting small values of M. Nevertheless it is possible with $M = 2$ paths to resolve consecutive peaks according to the Rayleigh criterion no matter how large the numbers to be factored.

It is amusing to consider the resources necessary to factor a 200-digit number which is considered really hard on a classical computer. From Eq. (9) we find for $\lambda_{min} \sim$ 100 nm the estimate $x \sim 10^{53}$ m which is much larger than the size of the universe [11] of 10^{27} m. Hence, such large numbers are not factorable with our method in the present form.

Obviously our analogue factorization algorithm does not provide an exponential speedup. Nevertheless it is very different from other classical algorithms which run on a digital computer. Indeed, in our case it is a physical phenomenon, that is interference, which we exploit to compute the factors of a given number. Although it is not possible to fully compare a digital with an analogue method we believe that our procedure paves the way for the use of physics for solving problems in number theory and we let "nature" solve complex problems for us.

[1] P. Shor, in: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, Nov. 20-22, 1994, IEEE Computer Society Press, pp. 124-134; L.M.K. Vandersypen *et al.*, Nature (London) **414**, 883 (2001); C.-Y. Lu *et al.*, Phys. Rev. Lett. **99**, 250504 (2007); B. P. Lanyon *et al.*, Phys. Rev. Lett. **99**, 250505 (2007).

[2] See for example R. Mack *et al.*, in *Mathematical Analysis of Evolution, Information and Complexity* edited by W. Arendt and W. P. Schleich (Wiley-VCH, Berlin, 2009).

[3] M. Stefanak *et al.*, J. Phys. A: Math. Theor. **41**, 304024 (2008).

[4] V. Tamma *et al.*, J. Mod. Opt. **56**, 2125 (2009).

[5] S. Wőlk *et al.* (unpublished); W. Merkel *et al.* (unpublished); W. Merkel *et al.*, Fortschr. Phys. **54**, 856 (2006); J.F. Clauser, and J.P. Dowling, Phys. Rev. A **53**, 4587 (1996); J. Summhammer, Phys. Rev. A **56**, 4324 (1997); A. A. Rangelov, J. Phys. B **42**, 021002 (2009); M. Stefanak *et al.*, New J. Phys **9**, 370 (2007).

[6] M. Mehring *et al.*, Phys. Rev. Lett. **98**, 120502 (2007); T.S. Mahesh *et al.*, Phys. Rev. A **75**, 062303 (2007); M. Gilowsky *et al.*, Phys. Rev. Lett. **100**, 030201 (2008); D. Bigourd *et al.*, Phys. Rev. Lett. **100**, 030202 (2008); M. Sadgrove, S. Kumar, and K. Nakagawa, Phys. Rev. Lett. **101**, 180502 (2008); S. Weber, B. Chatel and B. Girard, EPL **83**, 34008 (2008); X. Peng and D. Suter, EPL **84**, 40006 (2008).

[7] J.A. Jones, Phys. Lett. A **372**, 5758 (2008).

[8] M.V. Berry, Physica D**33**, 26 (1988); M.V. Berry and J. Goldberg, Nonlinearity **1**,1 (1988).

[9] We calibrate the spectrometer by using light sources with well known emission spectra such as mercury lines and sodium double D lines. The accuracy in the calibration of the spectrometer is high enough within the allowed experimental error.

[10] In our experiment there was no ambiguity in determining whether a dominant maximum is indeed located at an integer. Moreover, there was no need to normalize the output spectrum with respect to the source since the black body spectrum of the source is pretty constant in the measured bandwidth. However, for larger numbers we suggest the following strategy: (i) we first normalize the output pattern of the interferometer with respect to the intensity distribution of the source, (ii) then perform a best fit of the experimental pattern, and (iii) read out all the value of the maxima by using a standard peak finding procedure and check for a each number N to be factored if they correspond within the experimental accuracy in the wavelengths to an integer value of ξ_N. Since some non-factors may become indistinguishable from the values of the maxima in the interferogram we have to check if they actually divide N.

[11] C.H. Lineweaver and T. M. Davis, Sci. Am. **292**, 36 (2005).